UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,895	02/28/2002	Ted Christian Johnson	10017900-1	2863

22879   7590   09/04/2008
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
PEARSON, DAVID J

ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
09/04/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/085,895
Filing Date: February 28, 2002
Appellant(s): JOHNSON, TED CHRISTIAN

Daniel R. McClure
Reg. No. 38,962
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 06/17/2008 appealing from the Office action

mailed 01/31/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6092196	REICHE	7-2000
20020083178	BROTHERS	6-2002

6909708   KRISHNASWAMY et al.   6-2005

6490353   TAN   12-2002

6095418   SWARTZ et al.   8-2000

6110044   STERN   8-2000

Berners-Lee et al., RFC 1738, (Dec 1994), page 5

Verio Glossary Website. "P", (Oct 31, 2001), page 1

Schneier, Bruce. "Applied Cryptography" Second Edition, (1996), pages 56-65 and 183-

184

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 101

Claims 17-20 are rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter.

Claims 17-20 are directed towards a system. However the elements of the

"system" are logic. Page 15, lines 13-14 of Appellant's Specification says the logic can

be implemented in software. As a "system" composed entirely of software, the claim is

directed towards computer program, per se and is considered functional descriptive

material. Note MPEP 2106.01.

Claim Rejections - 35 USC § 103

Claims 1-2, 4-5, 8-13 and 17-24 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Reiche (U.S. Patent 6,092,196), and further in view of Brothers (U.S.

Patent Application Publication 2002/0083178).

For claim 1, Reiche teaches a method for authenticating a web session

comprising:

receiving a user ID (note column 10, lines 5-7);

computing a message digest of the user ID (note column 10, lines 19-20 and

column 12, line 24);

computing an expiration timestamp for the session (note column 10, lines 14-15);

combining the message digest and expiration timestamp (note column 10, lines

19-20);

encrypting a message using an encryption key (note column 10, lines 21-23);

and

converting the encrypted message into an ASCII string (note column 10, lines 23-

24).

Reiche differ from the claimed invention in that they fail to specify:

Selecting an index number;

Accessing an encryption key using the index number;

Brothers teaches:

Selecting an index number (note paragraph [0104]);

Accessing an encryption key using the index number (note paragraph [0104]);

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Reiche with the key index of Brothers. The combination of Reiche and Brothers would teach a system that selected a key using an index number (Brothers) and used the key to encrypt a URL message (Reiche). One of ordinary skill in the art at the time of the invention would have been motivated to combine Reiche and Brothers because it would increase security because using a different key for each session makes the same log in information appear different for each session, making it more difficult to break the encryption scheme or perform a replay attack.

For claim 17, the combination of Reiche and Brothers teaches a system for authenticating a transaction comprising:

Logic configured to receive a user ID (note column 10, lines 5-7 of Reiche);

Logic configured to compute a message digest of the user ID (note column 10, lines 19-20 and column 12, line 24 of Reiche);

Logic configured to select an index number (note paragraph [0104] of Brothers);

Logic configured to combine the message digest with expiration timestamp (note column 10, lines 14-20 of Reiche);

Logic configured to select an encryption key from a plurality of encryption keys using the index number (note paragraph [0104] of Brothers);

Logic configured to encrypt the combined message using the selected encryption key (note column 10, lines 21-23 of Reiche); and

Logic configured to convert the encrypted message into an ASCII string (note column 10, lines 23-24 of Reiche).

For claim 21, the combination of Reiche and Brothers teaches a method for authenticating a transaction comprising:

Computing a message digest of a user ID (note column 10, lines 19-20 and column 12, line 24 of Reiche);

Concatenating the message digest with an expiration timestamp (note column 10, lines 14-20 of Reiche);

Selecting an index number (note paragraph [0104] of Brothers);

Selecting an encryption key from a plurality of encryption keys using the index number (note paragraph [0104] of Brothers);

Encrypting the message digest using the selected encryption key (note column 10, lines 21-23 of Reiche); and

Converting the encrypted message into an ASCII string (note column 10, lines 23-24 of Reiche).

For claim 2, the combination of Reiche and Brothers teaches claim 1, wherein
the step of combining the message digest and expiration timestamp more specifically
includes concatenating the message digest and expiration timestamp (note column 10,
lines 19-21 of Reiche).

For claim 4, the combination of Reiche and Brothers teaches claim 1, wherein
the step of receiving the user ID more specifically comprises receiving the user ID
through an HTML page (note column 1, lines 60-65 of Reiche) that is communicated
from a remote client browser (note column 9, lines 27-30 of Reiche).

For claim 5, the combination of Reiche and Brothers teaches claim 1, wherein
the step of computing a message digest of the user ID more specifically comprises
computing a four-byte binary value which is an encoded form the user ID (note column
12, line 24 of Reiche).

For claim 8, the combination of Reiche and Brothers teaches claim 1, wherein
the step of accessing the encryption key more specifically comprises retrieving an
encryption key from a storage segment containing a plurality of encryption keys (note
paragraph [0165] of Brothers), wherein the retrieved encryption key is obtained from a
location or position within the storage segment based upon the index number (note
paragraph [0165] of Brothers).

For claim 9, the combination of Reiche and Brothers teaches claim 1, wherein the step of encrypting the combined message more specifically comprises encrypting the combined message digest and timestamp into an eight-byte value (note column 11, lines 51 and 53).

For claim 10, the combination of Reiche and Brothers teaches claim 1, further comprising the step of concatenating the index number to the encrypted message (note paragraph [0165] of Brothers).

For claims 11 and 13, examiner took Official Notice that the encrypted message is converted into an ASCII string using a "printf" command in Office Actions dated 02/15/2006 and 10/12/2006. Applicant did not traverse examiner's assertion and this statement is taken to be admitted prior art (note MPEP 2144.03).

For claim 12, the combination of Reiche and Brothers teaches claim 1, wherein the step of converting the encrypted message into an ASCII string more specifically includes converting the encrypted message into a hexadecimal value (note column 2, lines 24-26 of Reiche).

For claim 18, the combination of Reiche and Brothers teaches claim 17, further including logic configured to generate an expiration timestamp (note column 10, lines 14-15 of Reiche).

For claim 19, the combination of Reiche and Brothers teaches claim 17, further including logic configured to communicate the ASCII string to a remote computer (note column 10, lines 24-29 of Reiche).

For claim 20, the combination of Reiche and Brothers teaches claim 17, further including a local memory for storing the plurality of encryption keys (note paragraph [0165] of Brothers).

For claim 22, the combination of Reiche and Brothers teaches claim 21, wherein the step of encrypting the message more specifically includes encrypting the concatenated message (note column 10, lines 21-23 of Reiche) using the accessed encryption key (note paragraph [0104] of Brothers).

For claim 23, the combination of Reiche and Brothers teaches claim 21, wherein the step of selecting the encryption key more specifically includes retrieving the encryption key form a local memory based on the index number (note paragraph [0165] of Brothers).

For claim 24, the combination of Reiche and Brothers teaches claim 21, further including the step of communicating the ASCII string to a remote computer (note column 10, lines 24-29 of Reiche).

Claims 3, 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable

over the combination of Reiche and Brothers as applied to claim 1 above, and further in

view of Berners-Lee et al. and Verio.

For claim 3, the combination of Reiche and Brothers teaches claim 1, further

comprising passing the ASCII string to a remote computer within an HTML page (note

column 1, lines 60-65 of Reiche).

The combination of Reiche and Brothers differs from the claimed invention in that

they fail to specify the ASCII string is passed in an FTP URL being of the form

ftp://ID:ASCII@hostname, wherein ID is the user ID and ASCII is the ASCII string.

Berners-Lee et al. teach "URL schemes that involve the direct use of an IP-based

protocol to a specified host on the Internet use a common syntax for the scheme-

specific data: //<user>:<password>@<host>:<port>/<url-path>" They go on to specify

that <user> and <password> as "user: An optional user name. Some schemes (e.g.,

ftp) allow the specification of a user name. Password: An optional password. If present,

it follows the user name separated from it by a colon." (note section 3.1 on page 5)

The Verio glossary defines password as "A series of characters that enables

someone to access a file, computer or program." This definition would make the ASCII

value a password because it is a series of characters that are enabling a user to access

files on an FTP server.

It would have been obvious to one of ordinary skill in the art at the time of the

invention to combine the combination of combination of Reiche and Brothers with

passing the ASCII value in an FTP URL of Berners-Lee et al. One of ordinary skill in the art at the time of the invention would have been motivated to combine Reiche, Brothers and Berners-Lee et al. because it would provide a convenient way for a user to pass their user ID and password to a FTP server.

For claim 14, the combination of Reiche, Brothers and Berners-Lee et al. teach a method of claim 3, further including the step of passing the index number to the remote computer (note paragraph [0165] of Brothers).

For claim 15, the combination of Reiche, Brothers and Berners-Lee et al. teach a method of claim 14, wherein the step of passing the index number to the remote computer more specifically comprises passing the index number to the remote computer separate from the ASCII string (note paragraph [0019] of Brothers).

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Reiche and Brothers as applied to claim 1 above, and further in view of Krishnaswamy et al (U.S. Patent 6,909,708).

For claim 6, the combination of Reiche and Brothers differ from claimed invention in that they fail to specify the expiration timestamp is computed in Epoch format.

Krishnaswamy et al. teach a communication method that "records timepoints in the epoch time format." (note column 265, lines 37-46)

It would have been obvious to one of ordinary skill in the art at the time of the

invention to form the combination of Reiche and Brothers that computed the timestamp

in Epoch format of Krishnaswamy et al. One of ordinary skill in the art at the time of the

invention would have been motivated to combine Reiche, Brothers and Krishnaswamy

et al. because it would solve the problems associated with converting to and from

daylight savings time (note column 265, lines 37-46 of Krishnaswamy et al.).

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over the

combination of Reiche and Brothers as applied to claim 1 above, and further in view of

Tan (U.S. Patent 6,490,353).

For claim 7, the combination of Reiche and Brothers differs from the claimed

invention in that they fail to specify the index number used to access the encryption key

is randomly generated.

Tan teaches a key management scheme where "it may select these [key start

points and lengths] by randomly selecting table entry numbers."

It would have been obvious to one of ordinary skill in the art at the time of the

invention to combine the combination of Reiche and Brothers with the randomly

selected index numbers of Tan. One of ordinary skill in the art at the time of the

invention would have motivated to combine Reiche, Brothers and Tan because an

unpredictable sequence of encryption keys would decrease the likelihood of breaking

the encryption method.

Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over the

combination of Reiche and Brothers as applied to claim 21 above, and further in view of

Swartz et al (U.S. Patent 6,095,418).

For claim 25, the combination of Reiche and Brothers differs from the claimed

invention in that it fails to specify including the step of communicating the ASCII string to

a person through voice communication.

Swartz et al. teach communicating the ASCII string to a person through voice

communication (note column 4, lines 39-44).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to combine the combination of Reiche and Brothers with the spoken ASCII of

Swartz et al. to form a device which converted the message digest to ASCII and then

read the string aloud to someone. One of ordinary skill in the art at the time of the

invention would have been motivated to combine Reiche, Brothers and Swartz et al.

because it provide a convenient way to give the user their authenticated message

digest when they do not have access to a computer or an Internet connection.

Claims 26-28 rejected under 35 U.S.C. 103(a) as being unpatentable over the

combination of Reiche and Brothers as applied to claim 21 above, and further in view of

Stern (U.S. Patent 6,110,044).

For claims 26-28, the combination of Reiche and Brothers differs from the

claimed invention in that they fail to specify the ASCII string is printed onto a ticket

selected from the group consisting of an airline ticket, a concert ticket, an employee ID

card, and an event ticket and further specifying the ASCII string be printed on the ticket in a form that it may be later electronically scanned for verification.

Stern teaches a ticket printing and verification method which "contains a barcode printer (or other means for embodying a machine-readable indicium in a payout ticket), which prints both alphanumeric and barcode information on a payout ticket, including a validation number." (note column 3, lines 8-12) Note that in this case, a payout ticket would be an event ticket because successful verification of the ticket results in a payout event. Stern also teaches, "Selection circuitry 105 may also contain circuitry for encrypting all or part of the barcoded data imprinted on the payout ticket." (note column 4, lines 49-51)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Reiche and Brothers, which printed the ASCII string on an event ticket with a bar code of Stern. One or ordinary skill in the art at the time of the invention would have been motivated to combine Reiche, Brothers and Stern because it would provide a convenient and secure way to produce and verify the authenticity of a monetary winnings event ticket, which would be ideal for casino or other gaming companies.

Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Reiche, Brothers and Berners-Lee et al. as applied to claim 14 above, and further in view of Tan.

For claim 16, the combination of Reiche, Brothers and Berners-Lee et al. differs

from the claimed invention in that they fail to specify converting the encrypted message

into an ASCII string more specifically comprises converting a combination of the

encrypted message and the index number into an ASCII string, wherein the index

number is communicated to the remote computer as a part of the ASCII string.

Tan teaches a key management scheme where "the seed (randomly generated

index number) may be communicated as part of the message transmission."

It would have been obvious to one of ordinary skill in the art at the time of the

invention to combine the combination of Reiche, Brothers and Berners-Lee et al. which

includes the index number in the message transmission of Tan. One or ordinary skill in

the art at the time of the invention would have been motivated to combine Reiche,

Brothers, Berners-Lee et al. and Tan because it would provide a convenient way of

storing the index number so the server would not have to locally store which cookie is

encrypted with which key.

(10) Response to Argument

Claims 17-20: 35 USC 101 rejection

Appellant argues claims are in proper compliance of 35 USC 101 as reflected by

prior issued patents and Examiner's failure to initially rejection these claims (note Brief,

pages 5-7).

Examiner disagrees. While Examiner may have erred in not initially rejecting

claims 17-20, Examiner believes the current rejection of claims 17-20 under 35 USC

101 is in proper accordance with current Office policy regarding computer-related

subject for the reasons given above. As for issued patents using "logic" claim language,

claims are evaluated as statutory or non-statutory on a case by case basis. Examiner

refuses to comment on the validity of issued patents.

Independent claims 1, 17 and 21: 35 USC 103 rejection – Reiche in view of

Brothers

Appellant argues the rejection "ignores an expressly claimed feature" and "if

Reiche doesn't disclose accessing an encryption key using the index number, then

Reiche CANNOT disclose 'encrypting the combined message using the accessed

encryption key'" (note Appeal Brief, pages 8-9).

Examiner disagrees. Reiche teaches encrypting a message using an encryption

key (note column 10, lines 21-23) and Brothers teaches using an index to select a key

(note paragraph [0104]). The combination of Reiche and Brothers teaches every

limitation of independent claims 1, 17 and 21:

receiving a user ID (note column 10, lines 5-7, client ID of Reiche);

computing a message digest of the user ID (note column 10, lines 19-20 and

column 12, line 24 of Reiche; A cookie is constructed using the client ID. The cookie

contains a CRC checksum of the entire cookie, including the client ID. Note page 17,

lines 8-9 of Applicant's Specification teaches the message digest may be a checksum.);

computing an expiration timestamp for the session (note column 10, lines 14-15

of Reiche; The cookie used for the session includes an expiration timestamp.);

selecting an index number (note paragraph [0104] of Brothers; The sender uses a key index number to determine which key to use.)

combining the message digest and expiration timestamp (note column 10, lines 19-20 of Reiche; When the cookie is created, the different fields of the cookie are combined. These fields include an expiration timestamp (column 11, line 53) and the checksum or message digest (column 12, line 24));

accessing an encryption key using the index number (note paragraphs [0104] and [0127]-[0128] of Brothers; The sender uses key index number to determine which key to use.);

encrypting the combined message using the accessed encryption key (note column 10, lines 21-23 of Reiche and paragraph [0104] of Brothers); and

converting the encrypted message into an ASCII string (note column 10, lines 23-24 of Reiche; UUencoding is used to encode the message into ASCII format (note column 2, lines 24-26 of Reiche)).

Therefore, the **combination** of Reiche and Brothers teaches the claimed feature of "encrypting the combined message (Reiche) using the accessed encryption key (Brothers)." One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Appellant argues Reiche teaches away from using accessing an encryption key using an index number (note Appeal Brief, page 9).

Examiner disagrees. As appellant notes, Reiche teaches, "using a simple private key encryption algorithm." This statement of the embodiment of Reiche's system does not amount to a teaching away. Reiche does not criticize, discredit, or otherwise discourage the use of a multiple key system using an index to identify which key is being used. Also, Reiche does not teach away from a combination with Brothers because the same encryption algorithm used in Reiche could be used in the combination of Reiche and Brothers. Brothers teaches a method for using a plurality of keys and an index number to identify which key is used. However, once a key is selected, the same simple encryption algorithm could be used to perform the encryption of the combined message.

Appellant argues Brothers fails to teach "selecting an index number" and "accessing an encryption key using the index number" (note Appeal Brief, pages 9-11).

Examiner disagrees. Applicant has emphasized a few chosen sentences from the cited paragraph [0104]. However, applicant missed the sentence, "If more than one key is used in the system 10, the secure URL generator module can also append key index data indicating the key to be used…" Brothers further teaches in paragraphs [0127]-[0128] that key index number is used "to retrieve the appropriate key." Clearly, Brothers teaches "selecting an index number" and "accessing an encryption key using the index number."

Appellant argues Brothers is nonanalogous art (note Appeal Brief, pages 10-11).

Examiner disagrees. Appellant asserts "Brothers is not directed to authenticating a Web session" (note Appeal Brief, page 10). However, in the Background of the Invention found in paragraph [0003], Brothers states, "This invention is directed to a system for distributing a resource in a **network environment** for access by users on a restricted basis... Such resources can be activated or provided to a **user's web access device** upon **authentication and validation** of a request from such user's device" (emphasis added). Clearly, Brothers is directed to authenticating a Web session.

Assuming arguendo, Brothers were not directed to authenticating a Web session, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, the identification of the proper key to be used by a sending and receiving party.

Appellant argues the combination of Reiche and Brothers is improper because the combination "was not derived from the prior art itself, but rather from the Examiner's subjective viewpoint of a perceived benefit that would result IF the combination were made" (note Appeal Brief, pages 11-13).

Examiner disagrees. The motivation for the combination of Reiche and Brothers

did not come from "Examiner' subjective viewpoint", but from what was known to one of

ordinary skill in the art at the time of the invention. As evidenced by Schneier (Applied

Cryptography), a 1996 cryptography textbook, one of ordinary skill in the art at the time

of the invention would know session transmissions with varied keys would help prevent

replay attacks (pages 58-59) and cryptanalysis (pages 183-184).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the

Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/David J Pearson/

Examiner, Art Unit 2137

Conferees:

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137

/Matthew Smithers/
Primary Examiner, Art Unit 2137